CHELSEA	**CHELSEA LOGISTICS AND INFRASTRUCTURE HOLDINGS CORP.**	**INFORMATION SECURITY GROUP**	DOC CODE: IT IT-SECURITY-001
			Effectivity: 2023
INFORMATION SECURITY GROUP POLICY			Issue/Rev: 1 *Supersedes:*
Prepared by: Efren M. Bernardino Jr. Sr. I Head	**Reviewed by: Management Committee** **Recommended by:** **CHRYSS ALFONSUS V. DAMUY** President & CEO		**Approved by:** **Board of Directors** Chelsea Logistics and Infrastructure Holdings Corp.

1.0. Policy Statement

The field of Information Security has become increasingly critical in today's digital landscape, where the exchange and storage of sensitive information are paramount. As cyber threats continue to evolve and grow in sophistication, organizations and individuals alike are recognizing the need for robust protection and proactive measures to safeguard their data. This realization has led to the emergence of information security groups, dedicated teams of professionals who specialize in assessing vulnerabilities, implementing security measures, and responding to incidents to ensure the confidentiality, integrity, and availability of information.

2.0. Objective

The purpose of this Policy is to establish an Information Security Group (ISG) in compliance with SEC Memorandum "GUIDANCE FOR REGULATED ENTITIES ON ESTABLISHING AND MAINTAINING A CYBERSECURITY FRAMEWORK". The ISG will be responsible for ensuring the confidentiality, integrity, and availability of information in the processes of Chelsea Logistics and Infrastructure Holdings Corp. and its subsidiaries/affiliates.

Chelsea Logistics and Infrastructure Holdings Corp.'s subsidiaries include Chelsea Shipping Corp., Trans-Asia Shipping Lines, Incorporated, Worklink Services, Inc., Starlite Ferries, Inc., The Supercat Fast Ferry Corp., TASLI Services Incorporated and their subsidiaries.

Unless otherwise indicated, all references to "Chelsea Group" in this Policy shall mean Chelsea Logistics and Infrastructure Holdings Corp. and its subsidiaries/affiliates.

3.0. Scope

This Policy applies to all business units, work sites, business processes and systems, and business relationships within Chelsea Group.

This Policy is applicable to all Chelsea employees, clients, contractors and third-party vendors and other stakeholders (hereinafter referred to as 'Users') who have access to Company Information Assets.

3.1. Definition of Terms

Assets	Assets include information, systems, facilities, networks, and computers used by the Chelsea Group and Users.
Attacks	Refers to attempts to compromise the confidentiality, integrity and availability of computer data or systems or Assets.
Availability	An asset is available if it is accessible and usable when needed by an authorized entity.
Business Unit	Alternative term for a Chelsea Company.
Code of Conduct	Refers to the Chelsea Group of Conduct and includes all other policies and rules which may be issued regarding the safety and security of Assets.
Confidentiality	Refers to the obligation to protect and preserve information and ensure that it is not made available or disclosed to unauthorized entities.
Contractor	Refers to personnel who are contracted on a part time or temporary basis through loan staff/ staff augmentation engagements from external third parties. These personnel are not under Chelsea Payroll and generally operate out of Chelsea premises under the supervision of the Company's Management.
Cybersecurity	Refers to all activities associated with mitigating cyber risk, namely to identify, protect, detect, respond, and recover from cyberattacks. It shall likewise encompass protection of Assets from compromise

through the use—in whole or in part—of electronic digital media (e.g., computers, mobile devices or Internet protocol-based telephony systems).

Data Protection Officer (DPO)
Pertains to an individual designated by the entity to ensure compliance of the Personal Information Controller (PIC) or Personal Information Processor (PIP) with the Data Privacy Act of 2012, its Implementing Rules and Regulations, issuances by the National Privacy Commission (NPC) and other applicable laws and regulations relating to privacy and data protection.

Employee
Refers to personnel who are employed on a fulltime basis and are on the payroll of a Chelsea Company.

Incident Response Plan
Refers to the written plan that embodies a systematic approach taken to respond to and manage an Attack.

Information Security Incident
Made up of one or more unwanted or unexpected information security events that could very likely compromise the security of the Business Unit's information and weaken or impair its business operations.

Information System
Refers to computerized systems for the collection, organization, storage and communication of information.

Integrity
Refers to the accuracy and completeness of information and the methods that are used to process and manage it.

National Privacy Commission (NPC)
The government agency charged with the administration and implementation of the provisions of Republic Act 10173 known as the Data Privacy Act (DPA) of 2012.

Risk
Combination of the probability of an event and its consequence.

Security Operation Center (SOC)
The centralized function within a Business Unit employing people, processes, and technology to continuously monitor and improve its security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Segregation of
Concept of having more than one person required to complete a task,

Duties	where the separation by sharing of a single task by more than one individual is an internal control measure intended to prevent fraud and error.
Third Party Vendors	Refers to external organizations providing services contracted to the Chelsea Group, where the vendor personnel typically operate out of the Vendor's premises under the direct supervision of the Vendor management.
Threat	A potential event, when a threat turns into an actual event, it may cause an unwanted incident which may harm an organization or system.
User	Refers to all Chelsea employees, clients, contractors and third-party vendors and other stakeholders who have access to Company Information Assets.
Vulnerability Assessment and Penetration Testing (VAPT)	A technical security testing designed to identify and help address cybersecurity vulnerabilities.

4.0. Policy Guidelines and Procedures Responsibilities

The Information Security Group Policy has been issued under the authority of the Information Security Group (ISG) and has been approved by Management.

The ISG is responsible for the implementation, review, updating and monitoring compliance with this Policy.

5.0. Policy Compliance

Business Unit Heads and the ISG shall ensure compliance with this Policy and shall initiate and be responsible for the appropriate remedial action in all cases covered by the Policy.
Failure of employees to comply with this Policy shall result in disciplinary action in accordance with the provisions of the Chelsea Code of Conduct.

Any exception to this Policy will be handled in accordance with the 'Exception Procedure' provided herein.

6.0. Information Security Group

6.1. Information Security Group Table of Organization

Refer to **Annex "A"**

6.2. Information Security Group Membership

The roles and responsibilities of the Information Security Group and its members are as follows:

Information Security Group

The Information Security Group which is composed of selected members of the Chelsea Management Committee, that is, the President & CEO, CFO, and Department Heads specifically Legal, Strategic Communications, Security, HR, Audit, Risk Management and IT, shall have the following responsibilities:

- be responsible for Chelsea's Information Security Management System (CISMS). The Chief Information Security Officer (CISO) will lead the ISG in the CISMS Program;
- ensures that Chelsea's overall Information Security objectives and plans are met;
- recommends amendments to the Information Security Policy;
- provides appropriate direction, timely advice, guidance, and support to address any key information security concerns or issues reported by the team;
- provides necessary resources to support the development and/or implementation of organization-wide or site-specific information security management programs;
- approves and monitors major information security projects and budgets;
- approves exceptions to this Policy on a case-by-case basis in accordance with the 'Exception Procedure' provided herein;
- periodically provides updates on information Security activities to the Executive Committee and the Board of Directors;
- be responsible for the implementation, operation, monitoring, review, compliance, maintenance, and improvement of the CISMS program;
- be responsible for reviewing the Information Security Standards, Baselines, Procedures and Guidelines;
- reports exceptions/non-compliance with Information Systems Security Policy including

security incidents to the Executive Committee and, where required, to the Audit/Compliance Committee as well;

- ensures relevant training and Information Security awareness is provided to all key staff;
- actively responds to inquiries/information requested/audits conducted by regulatory authorities on matters relating to Information Security;
- monitors security and advises the Business Unit Heads about the security problems and violations/incidents, as and when they occur;
- perform periodic checks to ensure that an appropriate process exists for reporting security violations/incidents;
- approves the Annual Security Incident Report of Business Units prior to filing with the National Privacy Commission portal by the DPO.

Compliance Team

The Compliance Team which is composed of selected members of the Information Security Group, namely the Audit-DPO, Security and HR, shall have the following responsibilities:

- monitors and interprets relevant laws and regulations pertaining to Information Security, such as data protection laws (e.g., Data Privacy Act of 2012, GDPR, HIPAA), industry-specific standards (e.g., PCI DSS for payment card data), and other legal requirements.
- ensures that the Business Units' Information Security practices and policies are in line with the above-mentioned regulations.
- collaborates with the Information Security Group to develop and update Information Security policies, procedures, and guidelines, and works to ensure that these policies are communicated effectively throughout the Business Units and are being followed by all relevant stakeholders.
- responsible for coordinating and conducting internal and external audits to assess the Business Units' adherence to Information Security standards and regulatory requirements.
- works with third-party auditors and assessors to validate the Business Units' security posture.
- maintains accurate and up-to-date documentation related to Information Security practices, policies, assessments, and audits.
- provides regular reports to Management and other stakeholders about the Business Units' compliance status and any necessary remediation efforts.
- helps develop training programs and awareness campaigns to educate employees about Information Security best practices and compliance requirements and to create a

security-conscious culture within the Business Units.

- in the event of a security breach or incident, collaborates with the Information Security Group to ensure that the incident response plan follows regulatory and legal requirements.
- Coordinates with Strategic Communication in communication with regulatory authorities and affected parties, if necessary.
- evaluates and manages third-party vendors and service providers to ensure that their information security practices align with the Business Units' compliance requirements.
- works with the Information Security Group to continuously improve the Business Units' Information Security posture by staying updated on emerging threats, technologies, and regulatory changes.
- Reviews the Annual Security Incident Report of certain Business Units as required by the NPC and endorses to ISG for approval.

CHIEF RISK OFFICER

The VP Treasury/Deputy CFO is the Chief Risk Officer (CRO) who reports directly to the President & CEO on the implementation, operations and effectiveness of the Risk Management System. The CRO is responsible for the development and implementation of all risk management processes and methodologies. As such the CRO:

- leads the development, implementation of the Chelsea Risk Management Policy in accordance with the applicable standards for risk
- ensures that risk evaluation, monitoring, review and documentation occur in accordance with the Risk Management Policy and Methodology
- provides advice to the Board of Directors to ensure compliance with relevant legislation, regulations, policies and standards and to build Chelsea Group's capability to mitigate risk related to information, human, financial and physical resources
- produces a consolidated Risk Register approved by the President & CEO for submission biannually to the Audit and Risk Management Committee (ARMC) for review of limits of acceptable risk
- updates the Risk Profile Matrix, which provides an overview of risks and potential liability.
- ensures that a comprehensive financial control system is operating efficiently and effectively.

Business Unit Heads/Department's Representative for Information Security

Business Units Heads / Department's Representative for Information Security shall have the following responsibilities at their Business Units / work sites and locations:

- ensure that Information Security requirements as per the CISMS policies, standards, baselines, and procedures are implemented;
- ensure that the Business Unit's systems and processes operate in accordance with the Information Security policies and procedures;
- ensure risk management activities are carried out periodically;
- provide appropriate direction, timely advice, guidance, and support to implement the required Information Security control measures;
- investigate security violations/ incidents observed at the Business Unit / work sites and locations and initiate the appropriate disciplinary actions;
- ensure that relevant training and information security awareness is provided to all key Users;
- participate in ISG meetings and periodic Management review meetings headed by CISO;
- review and approve all Exceptions to this Policy prior to submitting the same to the ISG for final approval;
- actively support the Information Security Team during periodic ISMS audits/ reviews, approve corrective actions identified to close findings and track the same to closure.

Chief Information Security Officer (CISO)

The CISO / ISG lead is responsible for defining the Information Security Policies, Standards, Baselines, and Guidelines for the Chelsea Group. In addition, the CISO shall have the following responsibilities:

- liaisons with Information Security forums and Security Specialist to improve the Information Security posture within Chelsea;
- responds to inquiries/ information requested/ audits conducted by regulatory authorities on matters relating to Information Security;
- monitors security and advise the Business Unit Heads about the security problems and violations/ incidents, as and when they occur;
- performs periodic checks to ensure that an appropriate process exists for reporting security violations/ incidents;
- reviews the Information Security metrics and respond to critical Information Security Incidents identified within Chelsea;
- presents the Information Security audit results, communicate key Information Security

concerns and challenges and other Information Security Dashboards to ISG on a periodic basis;

- leads Cyber risk and Cyber intelligence, keeping abreast of developing security threats and help the Chelsea Group understand potential security problems;
- leads the Cyber Security Operations center, real-time analysis of immediate threats and triage when something goes wrong;
- plans, buys, and rolls out security hardware and software, and makes sure IT and network infrastructure are designed with the best security practices in mind;
- Keeps ahead of security needs by implementing programs or projects that mitigate risks;
- Determines what went wrong in a breach, dealing with those responsible if offenders are Chelsea employees, contractors or third-party vendors, and implements plans to avoid repetitions of the same crisis.

Information Technology (IT)

The IT comprises the Information Security Analyst and the Information Security lead appointed by the ISG and CISO, and shall have the following responsibilities:

- coordinates Information Security activities within the Business Units;
- supports the CISO and ISG in reviewing the Information Security Policies, Baseline, Standards, Procedures and Guidelines;
- responds to Information Security Incidents identified within the Chelsea Group and support the Information Security Officer while handling critical Information Security Incidents;
- performs periodic Information Security audits of Chelsea Information Security Management System and related processes;
- presents the Information Security audit results to the CISO and work with the ISG to track closure of the Information Security audit issues;
- measures the effectiveness and compliance of ISMS within the Chelsea Group;
- reviews the processes performed by the Information Technology team to ensure they are performed in compliance with this Policy and Information Security Procedures.

Security Operations Center (SOC)

- develops and designs security devices and software to monitor Information Systems utilized within Chelsea;
- monitors antivirus controls and solutions to ensure timely detection/ prevention, containment and recovery from attacks initiated by malicious code/software;
- prepares and maintains an authorized software whitelist and website whitelist;
- performs periodic security evaluations and testing on Information Systems to ensure they are hardened adequately;
- performs periodic Vulnerability Assessment & Penetration Testing (VAPT);
- periodically reviews the audit logs generated from IT systems to ensure timely detection and containment and management of Information Security events;
- monitors perimeter networks to ensure timely identification of suspicious activities, security events and breaches by malicious sources.

7.0 General Policies and Procedures

7.1 General Provisions:

The Information Security Group's responsibilities shall be formally allocated and accepted across the Business Units. In addition to the above, designated individuals shall be identified as owners for each Chelsea Information Asset.

The Information Asset Owner shall liaise with the Information Security Group and/ or application security leads to perform the following tasks:

a. Identifying the information assets and the security processes associated with each individual asset;
b. Classification and labeling of their respective assets in accordance with the 'Risk Management Policy and Methodology and Asset Management Policy and Procedure';
c. Risk management of their respective assets which involves identifying key risks, implementation of risk treatment plans and controls to protect assets and reduce the risk to an acceptable level, see 'Asset Inventory Register, Information Risk Register and Information Risk Treatment Plan'; and
d. Reviewing and approving user access privileges in accordance with the 'Access Control Policies and Procedures'.

All Users shall cooperate with Chelsea Information Security Group in implementing and maintaining Information Security controls. Users shall read, acknowledge and adhere to all

Chelsea acceptable usage policies while accessing Chelsea Information, Information Systems, and facilities.

7.2 Segregation of Duties

Roles and responsibilities of personnel handling Chelsea Information and/or Information Systems shall be defined to include appropriate segregation of duties in order to:

a. to reduce opportunities for unauthorized or unintentional modification or misuse of Chelsea's Information; and
b. to prevent fraud and potential malicious or accidental misuse of Chelsea's Information Systems.

7.3 **Confidentiality / Ownership**

This Information Security Group Policy is for the use of **Chelsea Logistics and Infrastructure Holdings Corp**. and its subsidiaries ('Chelsea').

The confidential and proprietary information contained herein shall not be disclosed, copied, or made available to anyone other than the process owners within Chelsea.

No part of this Policy may be reproduced or transmitted in any form by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system to external parties except as may be permitted in writing by Chelsea Management.

The Information Security Group identified in this Policy would be responsible for the management, implementation, monitoring, and compliance of the standards set herein and to address the inquiries or provide guidelines with regard to this Policy.

7.4 Exceptions

Exceptions to this Policy are likely to occur. Requests for exception must be made in writing addressed to President and CEO as Chairman of ISG and must contain:

- Name of the requestor
- The reason for the request for exceptions;
- Risk to the Business Unit of not following the written Policy;
- Specific mitigations that will not be implemented;

- Technical and other difficulties, and
- Date of review

8.0 Revision History

Each time this document is updated, this table should be updated.

.

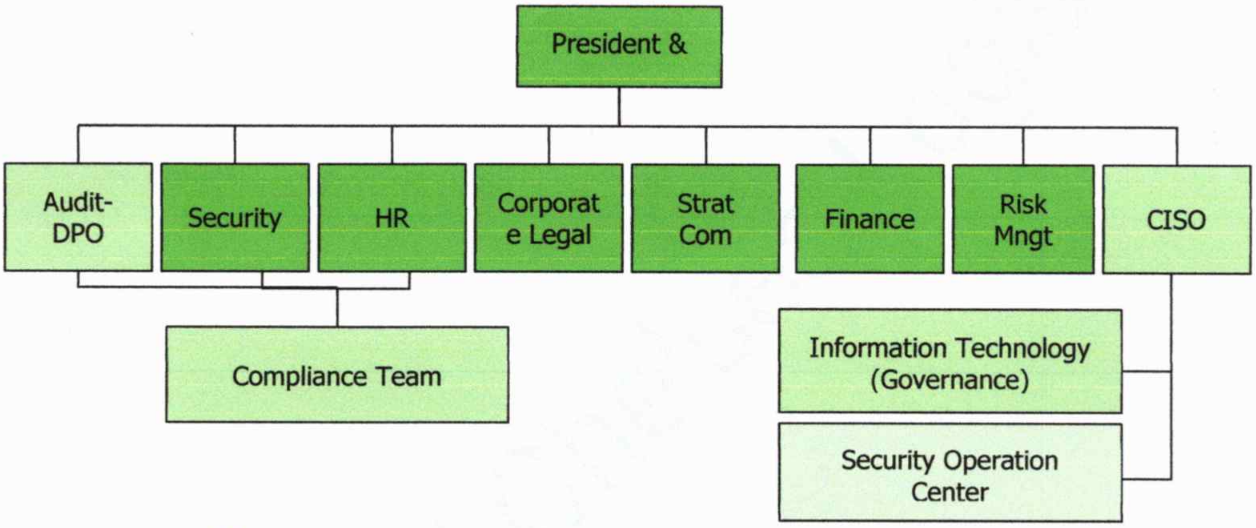
Version	Revision Date	Revision Description	Name
Draft	July 19, 2023	Draft core version	Efren M. Bernardino
Draft	July 26, 2023	Draft	Ma.Henedina V. San Juan
Draft	Aug 9, 2023	Draft	Katherine A. Agbay
Draft	Aug 10, 2023	Chief Risk Officer responsibilities	Reynaldo A. Phala
Draft	Aug 10, 2023	Compliance Team responsibilities	Efren M. Bernardino
Draft	Aug 15 2023	Edits	Katherine A. Agbay
Draft	Aug 16, 2023	Additional edits	Ma.Henedina V. San Juan
Draft	Aug 16, 2023	Additional edits	Sherlyn R. Guerzon
Draft	Aug 18, 2023	Remove the Application Security Head role/function	Efren M. Bernardino
Draft	Nov 11, 2023	Incorporate changes by Atty Dina San Juan	Efren M. Bernardino

Draft	Aug 18, 2023	Remove the Application Security Head role/function	Efren M. Bernardino
Draft	Nov 11, 2023	Incorporate changes by Atty Dina San Juan	Efren M. Bernardino

ANNEX A:

Information Security Group Table of Organization

INFORMATION SECURITY GROUP



APPROVED by the Board of Directors of Chelsea Logistics and Infrastructure Holdings Corp. at its 14 November 2023 meeting.

DENNIS A. UY
Chairman of the Board

CHRYSS ALFONSUS V. DAMUY
President & CEO